C.C.C.

Crypto Chasers Confidential

Enigma (ENG) Analysis

Type: Token

Circulating Supply: 74,836,171 ENG

Total Supply: 150,000,000 ENG

Marketcap: $179,747,503 USD

Whitepaper Style: Highly technical

Official Website

Coinmarketcap

Source Code

Whitepaper

About

Taken from their official website:

"The Enigma protocol is a second-layer, off-chain network that aims to solve the two biggest problems for blockchains: scalability and privacy. By enabling secure, decentralized data computation and exchange, Enigma allows blockchains to truly fulfill their powerful promise."

From the official whitepaper:

"A peer-to-peer network, enabling different parties to jointly store and run computations on data while keeping the data completely private. Enigma's computational model is based on a highly optimized version of secure multi-party computation, guaranteed by a verifiable secret-sharing scheme. For storage, we use a modified distributed hashtable for holding secret-shared data. An external blockchain is utilized as the controller of the network, manages access control, identities and serves as a tamper-proof log of events. Security deposits and fees incentivize operation, correctness and fairness of the system. Similar to Bitcoin, Enigma removes the need for a trusted third party, enabling autonomous control of personal data. For the first time, users are able to share their data with cryptographic guarantees regarding their privacy."

Enigma Team

Guy Zyskind: Co-founder & CEO (LinkedIn)

Co-founder & CEO
MIT Media Lab | 10+ years of software development

Guy's LinkedIn experience is shown on the next page:

Experience

Founder and CEO

Enigma MPC

June 2016 – Present (1 year 9 months) | San Francisco Bay Area

Analyze encrypted data using MPC and Blockchain technology

Research Assistant

MIT Media Lab

July 2014 – June 2016 (2 years) | Greater Boston Area

• Created Enigma - a Decentralized Computation Platform with Guaranteed Privacy. See: http://enigma.media.mit.edu. 100,000+ downloads of the whitepaper. Featured in WIRED, Wall Street Journal, FastCompany, Engadget, etc.
• Evangelizing Bitcoin/Blockchain and Cryptocurrencies research in academia.
• Making verifiable secure computation practical (Big Data analysis without seeing the data).

★ Thesis: Efficient Secure Computation Enabled by Blockchain
Technology

Instructor

Massachusetts Institute of Technology (MIT)

September 2015 – December 2015 (4 months) | Greater Boston Area

Taught MAS.S65 (Fall 15') - The first engineering class about bitcoin, blockchain and cryptocurrencies at MIT. See: http://blockchain.media.mit.edu.

CTO

Athena Wisdom

May 2012 – June 2014 (2 years 2 months)

• Led the establishment of an MIT spin-off company. Turned a decade worth of research into a scalable product and technology.
• Designed a scalable Big Data infrastructure capable of analyzing massive heterogeneous datasets from different data providers.
• Secured research collaborations with large enterprises, yielding breakthroughs in the study of complex systems and social interaction.

Co-Founder and CTO

Tamkix

June 2011 – December 2012 (1 year 7 months)

• Founded and implemented the company's main product Gripit, a location based real-time couponing system that allows businesses to attract nearby clients.
• Signed up over 150+ businesses in Tel Aviv alone for the initial beta.
• Featured several times on the local Apple's App Store most popular apps.

Co-Founder

CityOwls

December 2011 – November 2012 (1 year)

• Designed the core algorithms and data-mining agents, leading to the first global- scale sentiment-analysis of physical venues.
• Led the company to the prestigious 8200 EISP program, which only accepts 20 promising tech companies each year.

Software Developer

SAP

November 2009 – February 2012 (2 years 4 months)

• Innovated the first SAP Mobile Development Platform, which in one year became the group's flag product and the only product to do so in the past decade.
• Introduced advanced open source technologies, which significantly reduced operational costs and regulation.

Vice Editor-In-Chief, Director of Reviews

HWzone

November 2007 – November 2009 (2 years 1 month)

• Led Israel's largest IT news website to peak traffic rates, averaging around 150K+ unique page-views/day and around 40K readers per published article.
• Increased revenues from ads on every quarter. Established connections with senior product managers in the world's largest IT companies.

Education

Massachusetts Institute of Technology
Master of Science (M.S.), Media Lab, 5/5
2014 – 2016

Thesis: Efficient Secure Computation Enabled by Blockchain
Technology

Tel Aviv University
B.Sc, Electrical Engineering, Computer Science
2007 – 2011

The founder of Enigma seems to have a vast background in software development and even a masters from M.I.T. with his thesis on Blockchain. Overall, the large amounts of experience and his experience with blockchain in general seems like a very positive thing for the development of Enigma, and especially as a co-founder of this project.

Can Kisagun: Co-founder & CPO ([LinkedIn](#))

**Co-founder & CPO
MIT Sloan MBA | ex-McKinsey**

Can's LinkedIn experience is shown on the next page:

Experience

Co-Founder
Enigma MPC
Jan 2017 – Present • 1 yr 2 mos
San Francisco Bay Area

At Enigma, we enable anyone to build their own crypto-hedge fund. We are building Catalyst, an algorithmic trading tool and an investment platform for crypto-assets. Our short-term goal is to enable developers to build, test and master winning technologies. Over time we want to empower retail investors to invest in winning crypto-strategies through our platform

We are hiring! - https://goo.gl/forms/uHrTEFd32PQnOK433

Co-founder & CEO
Eximchain
Jan 2016 – Jan 2017 • 1 yr 1 mo
Boston

Eximchain builds international trade credit score for small to medium sized (SMEs) importers and exporters. Trust is built by transaction history and is key to global trade. However, SMEs lack a system that is widely accepted, globally adopted, and recognized as independent.

The rest of his experience includes a Product Manager intern at DataXu a programmatic marketing software, Founder & CEO of a startup called streetdust which is a mobile application for culturally intelligent street discoveries,

Education

Massachusetts Institute of Technology - Sloan School of Management
Master of Business Administration (M.B.A.)
2014 – 2016
Activities and Societies: - VP in MIT Sloan FinTech Club - MIT Bitcoin Club - Entrepreneurship and Innovation Club - Entertainment and Media Club - MIT Tech Club

Northwestern University
Bachelor of Science (BSc), Industrial Engineering & Management Sciences
2007 – 2011
Activities and Societies: - Completed Undergraduate Managerial Analytics Certificate by Kellogg School of Management - Won McCormick School of Engineering Award for Best Business Plan with a solar-energy venture in Africa

Co-founder & CEO
Eximchain
Jan 2016 – Jan 2017 • 1 yr 1 mo
Boston

Eximchain builds international trade credit score for small to medium sized (SMEs) importers and exporters. Trust is built by transaction history and is key to global trade. However, SMEs lack a system that is widely accepted, globally adopted, and recognized as independent.

Product Manager Intern
DataXu
Jun 2015 – Aug 2015 • 3 mos
Greater Boston Area

Programmatic Marketing software ranked #1 Demand Side Platform Offering in Forrester in 2015
- Analyzed impact of a beta campaign for a new product and ran pricing assessment
- Conducted market research to make a new product development decision based on market appetite and required technical level of effort

Founder & CEO
streetdust
Apr 2014 – Feb 2015 • 11 mos
Istanbul

Mobile application for culturally intelligent street discoveries
- Developed the product overseeing design, technical and content development workstreams
- Planned a cost-effective go-to market and customer acquisition strategies
- Instituted relationships with merchants and other tour operators to generate revenues through merchant partnerships and in-app purchases
- Pitched to top VCs in Silicon Valley as the finalist of MIT Sloan's Entrepreneurship & Innovation Club's Pitch competition

Business Analyst
McKinsey & Company
Sep 2011 – Apr 2014 • 2 yrs 8 mos

Advised clients primarily in media, banking sector studies and buy-side due diligence projects
• Created content buying optimization tool for a leading Turkish media group and improved revenue targets by 20% ($50M)
• Led client teams in magazine, radio and advertising sales departments of a leading media group in Turkey and identified operational improvement levers such as consolidation of processes, double hatting etc., corresponding to 10% savings
• Re-modeled credit approval levels and constructed a commercial credit analysis framework for a mid-sized Turkish bank, resulting in 30% reduction in non-performing loans ($35M)
• Moderated workshops in a leading global bank and coached division leaders in retail and commercial banking units to identify 15% personnel cost savings based on an efficiency benchmarking effort
• Built market sizing and revenue projection models for companies in Media, Health Care, Retail & Consumer Goods sectors to assess attractiveness of $1.3B investment
• Prepared a town-level expansion planning model for a Turkish retailer and identified locations of 200 new store openings

Education

Massachusetts Institute of Technology - Sloan School of Management
Master of Business Administration (M.B.A.)
2014 – 2016
Activities and Societies: - VP in MIT Sloan FinTech Club - MIT Bitcoin Club - Entrepreneurship and Innovation Club - Entertainment and Media Club - MIT Tech Club

Northwestern University
Bachelor of Science (BSc), Industrial Engineering & Management Sciences
2007 – 2011
Activities and Societies: - Completed Undergraduate Managerial Analytics Certificate by Kellogg School of Management - Won McCormick School of Engineering Award for Best Business Plan with a solar-energy venture in Africa

Volunteer Experience

Funding Advisor
#Tarih
Oct 2013 – Mar 2014 • 6 mos
Arts and Culture

#Tarih, formerly known as NTV Tarih, is a monthly magazine that covers historical events with contemporary relevance
- Formed a group of volunteer team of entrepreneurs and lawyers and led interactions between the volunteer team and the editorial team
- Developed a equity based micro-investment funding model to ensure editorial independence of the magazine
- Created a business plan and financial projections

Looking at this co-founder, it seems as if he also has a decent amount of past experience. Although not well versed in development and the blockchain as Guy, Can's experience deals more so within the business side, which pairs well with Guy's experience in development.

As both founders have a master from M.I.T., it can be said that they are both very educated in regards to their respective fields. With one having good development experience, and with the other having good business experiences, they both compliment each other as the head of this project.

TOR BAIR
Head of Growth and Marketing
MIT Sloan MBA | Former
options trader and data @
Snapchat

The third person listed on their website is Tor Bair - he's the head of growth and marketing and is easily accessible as we were able to easily talk to him via the Telegram chat.

Experience

Head of Growth and Marketing
Enigma MPC
2017 – Present • 1 yr

We closed our $45M ICO on September 11, 2017!

At Enigma, we want to re-think how data is shared, aggregated and monetized in a way that maximizes collaboration. That's why we are building the Enigma data marketplace protocol as well as Catalyst, the first application running on our protocol. Powered by our financial data marketplace, Catalyst empowers users to share and curate data and build profitable, data-driven investment strategies.

Data Scientist
Snap, Inc.
2016 – 2017 • 1 yr
Greater Los Angeles Area

Growth-focused projects including: broadcast and messaging behavior, user churn and retention, onboarding, international market analysis, competitive analysis

Revenue-focused projects including: ad performance, sponsored creative tools, auction / ads API implementation, advertiser retention

Tor has excellent experience as a Data Scientist at Snap, Inc. also with experience at other notable Silicon Valley companies such as HubSpot, Spotify.

His education like the others is very good:

Education

Massachusetts Institute of Technology - Sloan School of Management
Master of Business Administration (MBA)
2016
Activities and Societies: President of Rolling Sloans, Media Relations for Sloan Sports Analytics Conference

Coursework focusing on technology, analytics, media and art, social media, decentralization, messaging, communication, and collaboration. Media Lab coursework (Future Commerce, Blockchain Tech, Media Ventures) and associated projects.

Brown University
Bachelor's degree, Economics
2005 – 2009
Activities and Societies: Undergraduate Finance Board, Ultimate Frisbee, ARRR!!! Pirate A Cappella

Overall Tor seems to be a strong member and asset on the team.

Let's take at the development team listed on the official website:

VICTOR GRAU SERRAT
Senior Software Engineer
MIT D-Lab | 15+ years of
software development

FRÉDÉRIC FORTIER
Senior Software Engineer
Quant | 10+ years of software
development

## Victor Grau Serrat (LinkedIn) (GitHub)

Education: University of Maryland College Park B.S. in Electrical & Computer
Engineering: 2000 - 2003, Universitat Politècnica de Catalunya Masters in
Telecommunications/Electrical Engineering
Notable: Co-Director at MIT D-Lab : *D-Lab is an interdisciplinary program at MIT that is
building a global network of innovators to design and disseminate technologies that
meaningfully improve the lives of people living in poverty. Through academic offerings and
research projects, D-Lab seeks solutions that are low-cost and locally sustainable in fields such
as agriculture, water and sanitation, health, energy, housing and education.*

*Since joining the program in 2008, I shared its leadership in expanding its academic offerings
4x, growing its staff 10x, and increasing its operational budget 10x.*

518 contributions in the last year

Learn how we count contributions.
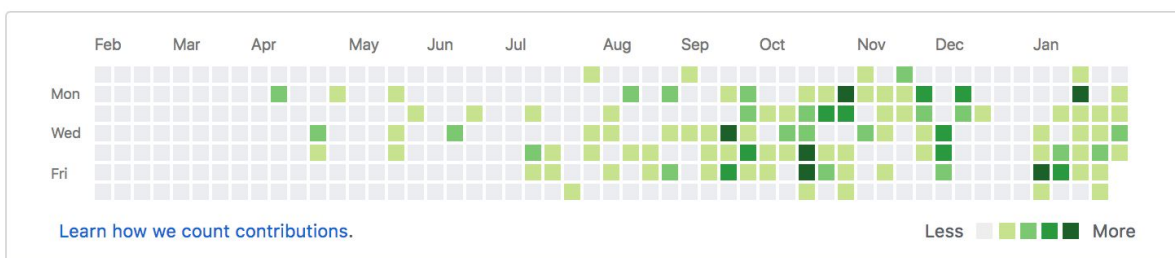
Contribution activity

Jump to ▾ | **2018**

February 2018

Created 29 commits in 2 repositories

enigmampc/catalyst 19 commits

enigmampc/marketplace 10 commits

2017
2016
2015
2014

In February so far he has 29 commits related to enigma - he is certainly an active
developer.

Frederic Fortier ([LinkedIn](#)) ([GitHub](#))

Education:

Education

Université de Sherbrooke
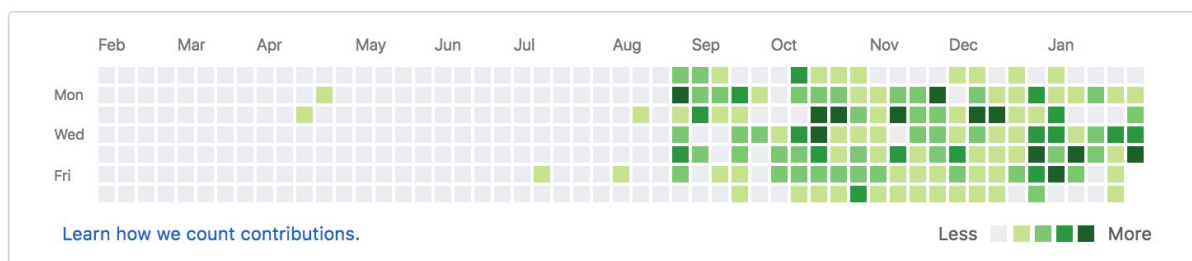Master of Science (M.Sc.), E-Commerce/Electronic Commerce
2004 – 2005

Université du Québec
Bachelor of Science - BS, Finance
2001 – 2004

Cégep Garneau
Diplome d'Etudes Collegiales, Computer Science
1998 – 2001

Notable: Multiple years of experience at various software companies such as enChoice Inc, Lighthouse Computer Services, BearingPoint, CIPC, and Imprimerie Quebecor Media Inc.

668 contributions in the last year

	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan
Mon												
Wed												
Fri												

Learn how we count contributions.   Less ▢ ▢ ▢ ▢ More

Contribution activity   Jump to ▾   **2018**

February 2018   2017

Created 39 commits in 1 repository   2016

enigmampc/catalyst 39 commits   2015

He's a very active developer with 39 commits in the enigmampc repository as of February.

It's nice to see that the website included their GitHub profiles - that's a very positive sign.

We rate the team as fundamentally strong based on the fact that there is active development a strong team of advisors as well as contributors.

You can view more about the team [here](#)

GitHub

On the next page we have included a screenshot of the GitHub - the last updated repository at the time of this writing was the catalyst repository which is a algorithmic trading library for crypto-assets in Python, the repo is quite active because it has 537 stars.

Here's a description of what Catalyst is:

Catalyst is an algorithmic trading library for crypto-assets written in Python. It allows trading strategies to be easily expressed and backtested against historical data (with daily and minute resolution), providing analytics and insights regarding a particular strategy's performance. Catalyst also supports live-trading of crypto-assets starting with three exchanges (Bitfinex, Bittrex, and Poloniex) with more being added over time. Catalyst empowers users to share and curate data and build profitable, data-driven investment strategies. Please visit enigma.co to learn more about Catalyst, or refer to the whitepaper for further technical details.

Catalyst builds on top of the well-established Zipline project. We did our best to minimize structural changes to the general API to maximize compatibility with existing trading algorithms, developer knowledge, and tutorials. Join us on Discord where we have a #catalyst_dev channel for questions around Catalyst, algorithmic trading and technical support.

catalyst

An Algorithmic Trading Library for Crypto-Assets in Python

`trading` `cryptocurrency` `cryptocurrencies` `algorithmic-trading`

● Python ★ 537 ⑂ 157 ⚖ Apache-2.0 3 issues need help Updated 2 minutes ago

marketplace

Data Marketplace documentation:
https://enigmampc.github.io/marketplace

`trading` `cryptocurrency` `cryptocurrencies` `algorithmic-trading`

Updated 7 hours ago

catalyst-docs

Documentation for the Catalyst algorithmic trading library

`documentation` `crypto` `trading-strategies` `trading-algorithms`

★ 38 ⑂ 5 ⚖ MIT Updated on Oct 31, 2017

enigmaslackbot

A simple FAQ answering bot for Enigma's Slack

● JavaScript Updated on Aug 20, 2017

catalystweb

Catalyst web-app

★ 3 Updated on Jul 28, 2017

slate

API Documentation v0.2

● JavaScript ★ 1 ⑂ 1 Updated on Mar 9, 2017

Top languages
● JavaScript ● Python

Most used topics
`algorithmic-trading`
`cryptocurrencies`
`cryptocurrency` `trading`

People   1 >

lacabra
Victor

Screenshot of the GitHub
Catalyst is actually a fork of [Zipline](#) another algorithmic crypto trading program.

Investors

Our Investors

Listed on their website are these list of current investors into the project. Unlike many other projects which have no backing, Enigma has some decently legitimate investors into the project which lends credibility to the whole project itself, and its progression further on into the future.

Whitepaper
Whitepaper is highly technical - this is expected as a big investor and contributor to this project is the Massachusetts Institute of Technology.
Here's an excerpt of the design overview:

Enigma is designed to connect to an existing blockchain and off-load private and intensive computations to an off-chain network. All transactions are facilitated by the blockchain, which enforces access-control based on digital signatures and programmable permissions. Code is executed both on the blockchain (public parts) and on Enigma (private or computationally intensive parts). Enigma's execution ensures both privacy and correctness, whereas a blockchain alone can only ensure the latter. Proofs of correct execution are stored on the blockchain and can be audited. We supply a scripting language for designing end-to-end decentralized applications using private contracts, which are a more powerful variation of smart contracts that can handle private information (i.e., their state is not strictly public). The scripting language is also turing-complete, but this is not as important as its scalability. Code execution in blockchains is decentralized but not distributed, so every node redundantly executes the same code and maintains the same public state. In Enigma, the computational work is efficiently distributed across the network. An interpreter breaks down the execution of a

private contract, as is illustrated in Figure 1, resulting in improved run-time, while maintaining both privacy and verifiability
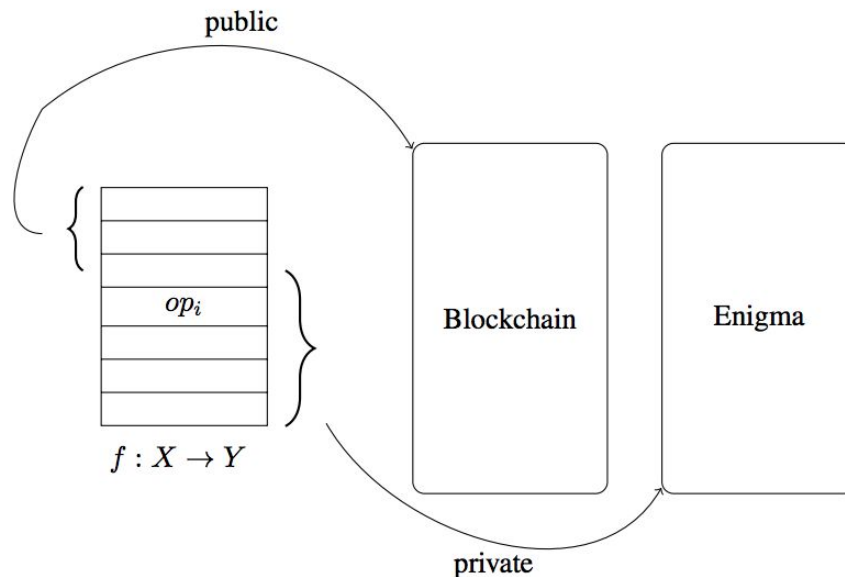

Figure 1: Code execution model.

Essentially what they're saying is that Enigma will serve as a network to load private computation off to and that public computations and results will be stored on the main blockchain.

4 Off-chain storage

Off-chain nodes construct a distributed database. Each node has a distinct view of shares and encrypted data so that the computation process is guaranteed to be privacy-preserving and fault tolerant. It is also possible to store large public data (e.g., files) unencrypted and link them to the blockchain. Figure 2 illustrates the database view of a single node.
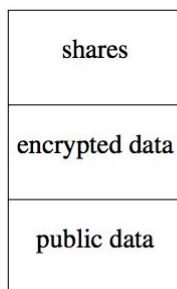

Figure 2: A node's local view of the off-chain data.

Here they talk about how they will be constructing a distributed database out of off-chain nodes.

The whitepaper is quite rigorous in its definition of secure multi-party communication (MPC) according to Wikipedia MPC is defined as:
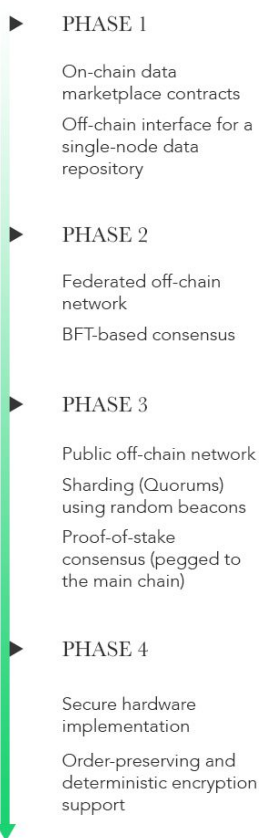
Secure multi-party computation (also known as secure computation, multi-party computation/MPC, or privacy-preserving computation) is a subfield of cryptography with the goal of creating methods for parties to jointly compute a function over their inputs while keeping those inputs private. Unlike traditional cryptographic tasks, where the adversary is outside the system of participants (an eavesdropper on the sender and receiver) the adversary in this model controls actual participants. These types of tasks started in the late 1970s with the work on mental poker, cryptographic work that simulates game playing over distances without requiring a trusted third party.

We appreciate the rigor in which the whitepaper was defined.

Roadmap

July 2017 — Summer 2017 — Q1 2018 — Q2-Q3 2018 — Q1 2019

Prototype
- Testing API
- Limited data sets

Token Sale

MVP
- Testing API
- Live trading
- Extended data sets
- Web UI / IDE
- Test net of Catalyst infrastructure

Catalyst 2.0
- Investment platform
- Single exchange   sign-on
- Community driven governance (data sets)
- Trading ICOs

Infrastructure
- Decentralized
- No custodian
- Coin agnostic

enigma

► PHASE 1

On-chain data marketplace contracts

Off-chain interface for a single-node data repository

► PHASE 2

Federated off-chain network

BFT-based consensus

► PHASE 3

Public off-chain network

Sharding (Quorums) using random beacons

Proof-of-stake consensus (pegged to the main chain)

► PHASE 4

Secure hardware implementation

Order-preserving and deterministic encryption support

Roadmap Information

Currently, the Enigma protocol is at the MVP stage of their roadmap, and are also following the phases shown on the left. In the first phase, the team will work on the foundation of Enigma on the on-chain portion for the data marketplace. The smart contracts dealing with this will be developed in Ethereum. At the second phase, they will work on a distributed off-chain network of nodes similar to side-chains to minimize the amount of threats in data loss.The third phase is when the team will release the open off-chain network for public to become part of the network of nodes. Within phase 4 is when the Enigma team will introduce "privacy features for protecting data in the network." This would allow the use to transfer data that may be private or confidential.

What's the deal with the $ENG token?

$ENG is a fixed ERC-20 token used to participate in the decentralized marketplace and also used for rewarding Enigma Catalyst traders.

Social Media

48.7K followers on their Twitter

9,970 readers on their Reddit

14,328 members on their Telegram

Notable News

Enigma just released their data marketplace on February 8, 2018.

Conclusion

Overall we rate Enigma as **fundamentally sound** due to their excellent team and active development as well as investors and partnerships. Although we rate Enigma as fundamentally sound it is also important to note that right now they're still in the minimally viable product stage which operates under a restricted threat model - which

means that they want to minimize the attack surface on their project while still growing their platform. As always we encourage potential investors to do their own research.

This document is certainly not an endorsement of Engima nor are we paid to promote them in any way - this information is publicly available and accessible by everyone we just put it here for convenience. That said, we encourage readers to stay cautious and look out for any scams or security issues associated with the coin.

References

Enigma Blog: https://blog.enigma.co/the-future-of-enigma-and-data-d5fb6ce450af